CS4471 Lab Assignment 3
Decoding Ethernet Frames

"*I hear and I forget; I see and I remember; I do and I understand*"

Go to web site http://www.wireshark.org and download a copy of the packet capture (sniffer) and analyzer for your VM instance of Windows operating system. (7 pts for each question)

1. Turn on your sniffer in promiscuous mode and begin capturing all network traffic.

   a. What is the destination Ethernet address of broadcast traffic? Submit screenshot with this value circled.

   b. What is the destination IP address of broadcast traffic? Submit screenshot with this value circled.

   c. What filtering rule can you use on your sniffer so that it will display only Ethernet frames that contain your computer's IP address? Submit a screenshot with this filter in effect.

   d. What filtering rule can you use on your sniffer so that it will display only Ethernet frames that contain your computer's Ethernet address in the Ethernet frame header? Submit a screenshot with this filter in effect.

2. Capture and decode an **ARP request** and the corresponding **ARP reply** packet. You may need to initially clear your ARP cache (arp –d) in command prompt window (cmd.exe) before generating an ARP packet.

   a. a. What is the hexadecimal value the field in Ethernet frame header that is used to identify that the packet is an ARP packet? Submit screenshot with this value circled.

   b. Turn in screenshots which show the two types of ARP packets decoded.

3. Capture and decode an **ICMP echo request** and the corresponding **ICMP echo reply** packet by running the ping command.

   a. What is the decimal value of the protocol field in IP header that is used to indicate that the packet is an ICMP packet? Submit screenshot with this value circled.

   b. Turn in screenshots which show the two types of ICMP packets decoded.

4. On your Windows computer, capture and decode packets generated by a tracert command from your lab computer to www.calstatela.edu.

   a. What does tracert command do to its ICMP packets that will cause the routers to reply with ICMP messages?

   b. Turn in screenshots which show tracert packets decoded.

5. Capture and decode packets associated with a http session. Provide screenshots to support your answers.

   a. Circle and Identify the packets on a screenshot that comprise the 3-way handshake used during startup of the TCP connection. What TCP flags were set to 1 during the 3-way handshake?

   b. What were the absolute and relative values of the initial sequence numbers used by the http client and server? Submit screenshots with these values circled.

   c. What tcp port numbers did the web client and server use? Submit screenshot with these values circled.

   d. What were the absolute and relative values of the final acknowledgement numbers sent by the http client and server? Submit screenshots with these values circled.